REMARKS

This application has been carefully reviewed in light of the Office Action dated January 25, 2005. Claims 1 to 3, 6, 7, 10 to 14, 18 to 20 and 22 to 28 are pending in the application, of which Claims 1, 10, 14, 18, 20 and 22 are independent. Reconsideration and further examination are respectfully requested.

Applicant wishes to thank the Examiner for the courtesies and thoughtful treatment accorded Applicant's undersigned representative during the June 20, 2005 telephonic interview. This Amendment has been prepared based on the discussions and agreements reached during that interview.

In more detail, during the interview, the outstanding rejections were discussed in which Claims 1 to 3, 6, 7, 10 and 12 to 14 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,619,015 (Hickman) in view of U.S. Patent No. 6,192,473 (Ryan), Claims 2 and 11 have been rejected under 35 U.S.C. § 103(a) over Hickman in view of Ryan and further in view of Official Notice, Claims 18 to 20 and 22 were rejected under 35 U.S.C. § 103(a) over Ryan in view of Schneier ("Applied Cryptography"), Claims 23 to 25, 27 and 28 were rejected under 35 U.S.C. § 103(a) over Hickman in view of Ryan and further in view of U.S. Patent No. 5,534,857 (Laing), and Claim 26 was rejected under 35 U.S.C. § 103(a) over Ryan in view of Schneir and further in view of Laing. Specifically, Applicant's undersigned representative and the Examiner discussed clarification of the present invention's feature of the image input apparatus (e.g., a digital camera or digital scanner) generating a digital image, connecting a key storage device to the image input apparatus such that a key used for encrypting the generated image is read from the connected key storage device, is stored in the apparatus and is used to encrypt the digital image, after which the key is erased. The encrypted image is stored in the apparatus

such that, at some later time, when a user wants to retrieve the encrypted image, they connect the key storage device to the apparatus so that a decryption key is read from the device and is used to decrypt the encrypted image. Thus, a stand alone device, such as a digital camera or scanner, can be used to generate, encrypt and store a digital image, but the encryption key is maintained in an external storage medium that is locally connected to the device and the key is only temporarily stored in the device and is erased once the image is encrypted, thereby preventing a hacker from obtaining the key and decrypting the image. Thus, it was agreed during the interview that clarification of the foregoing features in the claims would overcome the outstanding rejections.

Accordingly, the claims have been amended in accordance with the interview and Claim 1 now recites an image input apparatus comprising connecting means for locally connecting a key storage device to the image input apparatus, generating means for generating a digital image in the image input apparatus, reading means for reading an encryption key stored in the key storage device connected to the connecting means, storage means for storing, in the image input apparatus, the read encryption key to execute an encryption process, encryption means for encrypting the generated digital image with the encryption key stored in the storage means, output means for outputting the encrypted digital image to a memory in the image input apparatus, erasing means for erasing the encryption key stored in the storage means after encrypting the digital image by the encryption means, obtaining means for obtaining, from the key storage device, a decryption key corresponding to the encryption key, and decryption means for decrypting the stored encrypted digital image by using the decryption key obtained by the obtaining means.

Amended independent Claims 10 and 14 are method and program claims, respectively, that substantially correspond to Claim 1.

Amended independent Claim 18 includes features along the lines of Claim 1, but includes additional features relating to encryption of an internal key using the key from the locally connected key storage device. Thus, Claim 18 is an image input apparatus comprising connecting means for locally connecting a key storage device to the image input apparatus, image generating means for generating a digital image in the image input apparatus, key generating means for generating an internal key, image encryption means for encrypting the generated digital image with the internal key, reading means for reading an encryption key stored in the key storage device connected to the image input apparatus, storage means for storing, in the image input apparatus, the read encryption key to execute a key encryption process, key encryption means for encrypting the internal key with the read encryption key stored in the storage means, output means for outputting the encrypted digital image and the encrypted internal key to a memory in the image input apparatus, erasing means for erasing the read encryption key stored in the storage means and the internal key after executing the encryption process by the image encryption means and the key encryption means, obtaining means for obtaining, from the key storage device, a decryption key corresponding to the read encryption key stored in the key storage device, key decryption means for decrypting the encrypted internal key with the obtained decryption key, and decryption means for decrypting the encrypted digital image with the internal key decrypted by the key decryption means.

Amended independent Claims 20 and 22 are method and program claims, respectively, that substantially correspond to Claim 18.

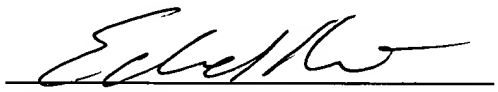
As discussed during the interview, the applied are is not seen to disclose or to suggest at least the feature of locally connecting a key storage device to a image input apparatus, reading an encryption key stored in the locally connected key storage device and

storing, in the image input apparatus, the read encryption key to execute an encryption process, encrypting a digital image generated by the image input apparatus with the stored encryption key, and erasing the stored encryption key after encrypting the digital image. Thus, each of amended independent Claims 1, 10, 14, 18, 20 and 22, as well as the claims dependent therefrom, are believed to be allowable.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant
Edward A. Kmett
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 98137v1